Dept. of Homeland Security Science & Technology Directorate

Secure Wireless Data Communications Trial

NIST IBE Workshop
Gaithersburg, MD
June 3, 2008

Douglas Maughan, Ph.D.
Program Manager, CCI
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170

Homeland Security

DEFENCE R&D DÉFENSE

Science and Technology (S&T) Mission

Conduct, stimulate, and enable **research, development, test, evaluation and timely transition** of homeland security capabilities to federal, state and local operational end-users.

What is the CA-US Public Security Technical Program (PSTP)?

- Bi-lateral program to develop and implement cooperative programs addressing S&T priorities for Critical Infrastructure Protection and Border Security
  - Systems engineering approach provides strategic focus on most important capability needs
  - Uses a top-down methodology for program direction and development
  - Supported by a government-to-government framework Agreement that enables CA-US coordination and collaborative work on common S&T priorities
- Leverages and builds on existing collaborations and programs

Homeland Security

3

Program Participants

Program Lead	Homeland Security	DEFENCE R&D DÉFENSE
Government Participants	DHS Science & Technology Cyber Security R&D CENTER	DEFENCE R&D DÉFENSE Secure Mobile Networking Group
Industry Participants	CipherTrust Voltage	Entrust EMS SATCOM

Homeland Security

3 June 2008 4

Objective of the DHS Secure Wireless Data Communication Trials

- Evaluate and demonstrate cross-border interoperability of secure data communications architectures using commercially available wireless technologies and devices that will allow us to achieve our mission
- Use results of the program to improve the secure delivery of critical information via the wireless technologies used by public safety, emergency preparedness, and law enforcement communities of Canada and the United States

Research Questions

- Infrastructure-level research
  - What solutions provide technology for cross-border mobile data encryption?
  - What new technologies can be used for public key cryptography different from traditional public key infrastructures?
- Device-level research
  - How does enhanced security affect usability?
  - How can security be enforced by improved policy or procedure?

In a Perfect World …

- All e-mail would be protected and be safe:
  - Be signed and encrypted
  - Conform to organizational policies
  - Be safe from malware and unpredictable behavior
  - Reliable everywhere
- *But we don't live in a perfect world!*
  - Traditional PKI is difficult
    - http://elib.tu-darmstadt.de/diss/000682/tstraub_diss.pdf
  - Encrypted messages prevent content inspection
  - Users will attempt to circumvent technical controls
  - Written policies are hard to enforce

First Issue: Traditional PKI

- Signing is easy
- Administration of Certificate Authority (CA) is time consuming
  - Okay for big corporations, but not for small organizations like local police departments
- Revocation lists are unwieldy
- Root CA proliferation
- Encryption to new users is hard
  - Especially on a mobile device

1st Encryption Alternative
Identity Based Encryption

- Retrieval of encryption parameters is based on an identity
  - For e-mail, the identity is the email address
  - Other attributes can be used to establish an identity
- Management is simplified
- Encryption is easy, even if the recipient has not yet been created

2nd Encryption Alternative
Assisted PKI

- Off-loads some work from sender
- Messages are sent encrypted to a server instead of the recipients
- Server is responsible for requesting and processing certificates
- E-mail message is then re-encrypted for the end recipients

Second Issue: Content Scanning

- Encrypted malware renders traditional scanners useless
  - Viruses, phishing attacks, and embedded malware reach the end users unchecked
- Compliance checking is also rendered ineffective when messages are encrypted
- Scanning is not just for malware but also for policy violations
- Centralized content scanning important
  - Reduces end user training requirements
  - More robust and capable
  - End user is unable to circumvent

Homeland Security

Third Issue: Availability

- Man-made and natural disasters limit coverage at worst possible time
- Many needed regions have no cell coverage
  - Much of the Mexican and Canadian borders
  - Along the coasts
- Canadian counterparts are investigating satellite technology

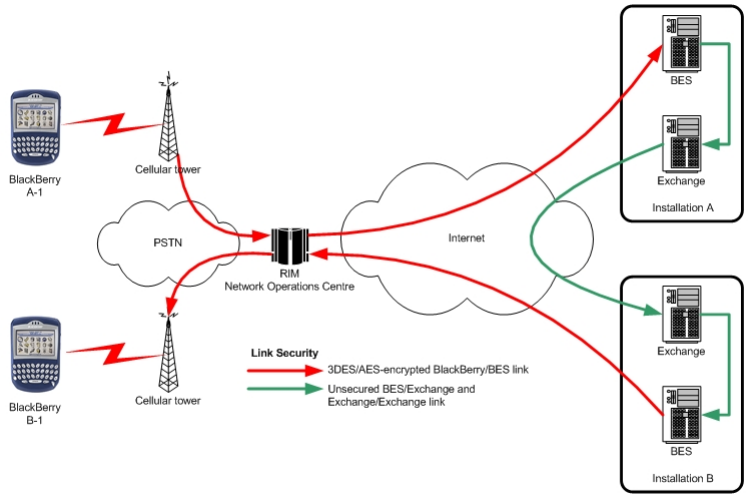
Homeland Security

DHS Secure Wireless Trials

- Encryption Technologies
  - S/MIME Support Package - Research in Motion (RIM)
  - Identity Based Encryption - Voltage Security
  - Assisted PKI - Entrust's Messaging Server
- Content Scanning Technologies
  - CipherTrust's IronMail Server
  - Entrust's Compliance Server
- Messaging Technologies
  - RIM Blackberry Handheld and Blackberry Enterprise Server
  - Microsoft Exchange Server

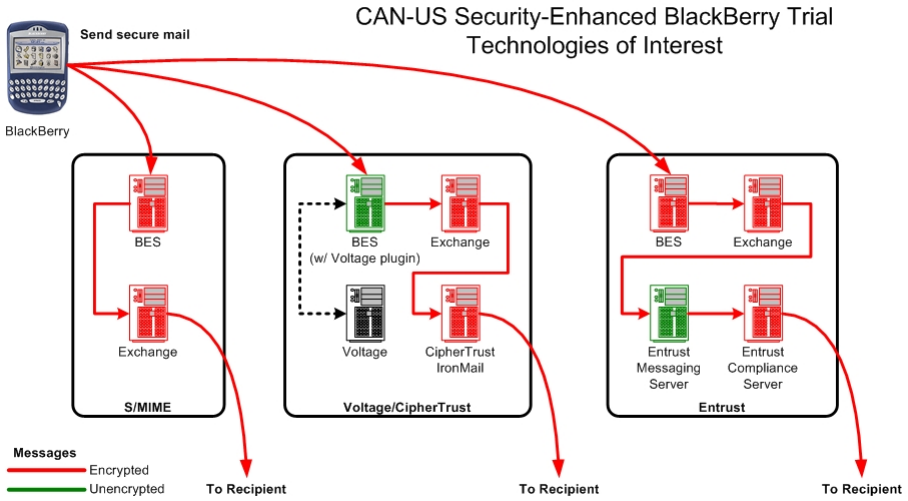
Homeland Security

Traditional Architecture



Homeland Security

Trial Architecture



Homeland Security

US-Canada Joint Trial

- Objective
  - Test effectiveness of CAN/US cross-border architecture to enable real-time communication in a variety of scenarios
- Trial Activity
  - Several trials over about a year with automated messaging activities and 30+ users acting out homeland security scenarios

Washington DC - 11 users (7 users in Washington DC, networked connection to 3 users in Atlanta and 1 user in New Mexico)
Menlo Park, CA - 11 users (10 full-time users, 1 test device)
Ottawa - 20 users (all full-time users)

Homeland Security

Trial Findings: Device Protection

- Users found that passwords and content protection did not significantly affect their experience
- Ability to kill device remotely worked well
- Activation over the air was not quick (15 minutes) but generally worked well

Trial Finding: Encryption Usability

- Users found that Voltage was very easy to use
- S/MIME not easy to use
  - Importing certificates was time consuming and frustrating
  - Some users never successful and dropped from experiment
  - Larger message size due to ciphertext and certificate forced doing a 'More All' before being able to read messages

Usability Survey Results

	Encrypted Email User Survey	S/MIME		VOLTAGE	
		18-Oct	19-Oct	18-Oct	20-Oct
1	I was able to read messages (7: with ease; 1: with difficulty)	4.15	5.56	6.38	6.70
2	I was able to send messages (7: with ease; 1: with difficulty)	3.69	5.11	6.63	6.90
3	Sending an email to a new recipient was (7: easy; 1: difficult)	2.46	4.25	6.75	6.89
4	Sending and receiving encrypted makes me feel (7: more secure; 1: less secure)	5.69	6.11	5.38	5.30
5	If I had the choice, I would (7: turn on encryption capability; 1: turn it off)	4.23	5.11	6.00	6.40
	Average end-user opinion after each product trial (questions are not weighted)	**4.04**	**5.23**	**6.23**	**6.44**
		57.47	**73.74**	**88.54**	**91.22**

Retrieving another's PKI certificate on a BlackBerry

Trial Findings: Policy Enforcement

- IronMail correctly identified all Voltage-encrypted emails containing social security numbers in the body of the message or in zipped and Word format attachments
  - Oddly formatted Word documents prevented properly enforced policy (vendor fixed immediately)
- IronMail correctly identified and quarantined Voltage-encrypted e-mails containing viruses in zipped and unzipped attachments

Trial Findings: Advanced Policy Enforcement

- Six policies
  - Configured by CipherTrust and Entrust personnel
- Policy enforcement is an iterative process
  - Difficult to decide what should be protected
  - Difficult to convey to a third party those decisions
  - Difficult to implement decisions into rules
    - Slight variations in text often fools rules
    - Synonym permutation explosion
- Correctly parsed about 60% of messages
  - Some instructions misunderstood
  - Some rules misconfigured

Trial Findings: Discoveries

- Message receive times varied greatly
  - Side by side BlackBerrys from the same mail domain received messages up to 30 minutes apart
  - Possible loss of MAPI connection between BES and Exchange server
- S/MIME key management for external users was much more difficult than expected
  - Some S/MIME participants were not able to get up and running
- Great care needs to be taken to set up policies
- No audio notification of loss of voice or data connectivity
- Cannot simultaneously use voice and data communications

IBE-to-S/MIME Conversion

- Voltage and Entrust have web mail capabilities for secure e-mail communication with individuals w/o their technology
- Web mail is not seamless
- Voltage added capability to also perform S/MIME encryption
- Testing Method
  - Internal user used only Voltage IBE technology: BlackBerry, Outlook client w/ Voltage, and ZDM (web mail)
  - External user used only S/MIME encryption
  - Internal user's S/MIME private and public certificates placed on Voltage server
  - External user's S/MIME public certificate placed on Voltage server
- Worked seamlessly!

Integrating Technology into Government

- What is the mobile data device strategy across government?
  - Agencies are using multiple devices (e.g. BlackBerry, Siemens)
- What is the process for integrating new technology into government architecture?
  - Understanding requirements
  - Getting approval
- What role do agencies have in sponsoring trials and how should the results be disseminated?

Douglas Maughan, Ph.D.
Program Manager, CCI
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170

For more information, visit
http://www.cyber.st.dhs.gov

Homeland Security